Strategisches Vorgehen

Das IT-Sicherheitskonzept

Wer hat wann zu welchen Daten Zugriff?

Die Grundlagen für jede IT-Umgebung sind ein IT-Konzept und darauf aufbauend ein IT-Sicherheitskonzept. Beide Dokumente sind von der Firmenstrategie abgeleitet.

Das IT-Sicherheitskonzept beschreibt die notwendigen Massnahmen zur Realisierung und Aufrechterhaltung des für das Unternehmen angemessenen, definierten Sicherheitsniveaus. Das IT-Sicherheitskonzept betrifft alle Stufen: Die Geschäftsleitung ist ebenso beteiligt wie die IT-Leitung, die IT-Abteilung und die Mitarbeiter. Sollte einer der Genannten nicht an Bord sein, droht schon hier der Keim des Scheiterns.

Damit ein IT-Sicherheitskonzept erstellt werden kann, müssen vier Fragen beantwortet werden:

1. Was will ich schützen?
2. Wogegen soll ich mich schützen?
3. Wie kann ich diesen Schutz erzielen?
4. Kann ich mir diesen Schutz leisten?

Die Frage nach dem Schutzbedarf
Die erste Frage gilt dem Schutzbedarf. Was will ich schützen? Die drei Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit helfen, diese Frage zu beantworten.

Die Verfügbarkeit gibt an, welche Systeme, Prozesse, Abläufe und Personen für welche Situation zur Verfügung stehen müssen. Unter der Integrität wird die Unversehrtheit der Daten verstanden. Die Vertraulichkeit schützt die Daten vor fremden Blicken. Immer wichtiger wird der vierte Grundwert: die Nicht-Abstreitbarkeit. Es muss klar ersichtlich sein, wer etwas gemacht beziehungsweise verändert hat.

Die Frage nach dem Wogegen
Ein Unternehmen muss sich klar sein, welche Gefährdungen einwirken können und ab welchem Punkt ein Schaden bedrohlich wird. Hier gilt es, verschiedene Szenarien und die Folgen abzuschätzen. Dies können zum Beispiel Stromausfall, Wassereinbruch, Mitarbeiterabsenz, Systemabsturz, Malware, Hacker oder Sabotage sein. Die Grundschutzkataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik) zählen eine Vielzahl von weiteren Gefährdungen auf.

Massnahmenauswahl einleiten
Aus dem Schutzbedarf und der Risikoanalyse leiten sich Massnahmen ab und weitere strategische Fragestellungen. Welche Massnahmen sind möglich? Damit auch verbunden, welche Gefährdungen kann eine einzelne Massnahme abdecken? Hat diese allenfalls Einfluss auf andere Gefährdungen oder Massnahmen? Welche Bereiche werden zusätzlich tangiert? Je nachdem, welche Bereiche abgedeckt werden, sind mehr Personen, eventuell sogar Externe involviert, oder es müssen allenfalls Prozesse angepasst werden. Eine zentrale Frage ist auch der Nutzen. Was bringt es mir, wenn ich eine Massnahme umsetze? Habe ich anschliessend die Ressourcen, diese Massnahme aufrechtzuerhalten?

Inhaltsverzeichnis eines IT-Sicherheitskonzeptes

- **Grundlage, Zweck**
  Die Einleitung beschreibt die Grundlagen der Firma, die Infrastruktur und die vorhandenen Mittel (Infrastruktur, Mitarbeiter und Prozesse).

- **Anforderungen Infrastruktur**
  Die Anforderungen an eine Infrastruktur sind zahlreich. Jede Abteilung hat andere Ansprüche an die Umgebung. Daher ist es sinnvoll, die Funktionen und Prozesse über alle Stufen aufzuschreiben.

- **Anforderungen Sicherheit**
  Mit diesen Anforderungen leiten sich die Bedürfnisse an die (IT-) Sicherheit ab.

- **Sicherheitsorganisation**
  - **Zuständigkeiten**
    Die Sicherheit gehört in den Zuständigkeitsbereich der Geschäftsleitung. Die Verantwortung kann gemäss Gesetz nicht delegiert werden. Jedoch können weitere Stellen bestimmt werden, die für (Teil-)Bereiche zuständig sind und gegenüber der Geschäftsführung Bericht ablegen.
  - **Rahmen für die Informations-Sicherheit**
    Das IT-Sicherheitskonzept muss von der Geschäftsleitung initiiert werden. Die IT-Leitung erstellt Anforderungen an die Informatik-Umgebung und schlägt Lösungen vor. Diese werden durch die Geschäftsleitung genehmigt.
  - **Pflege und Wartung des Sicherheitskonzepts**
    Die Anforderungen an eine IT-Infrastruktur wechseln ständig. Auch das Umfeld der Firma ändert sich sehr schnell. Das IT-Sicherheitskonzept muss den veränderten Bedingungen Rechnung tragen.

- **Sicherheit beim Personal**
  - **Vertraulichkeitsvereinbarung**
    Informationen der Firma gehören auch der Firma und stellen das Potenzial beziehungsweise den wirtschaftlichen Vorteil gegenüber Mitbewerbern dar. Dieses Wissen muss geschützt werden. Alle Mitarbeiter werden schriftlich zur Vertraulichkeit verpflichtet.
  - **Mitarbeiterausbildung in Sicherheitsfragen**
    Nur was bekannt ist, kann auch gelebt werden. Die Mitarbeiter sind in regelmässigen Abständen zu sensibilisieren.
  - **Reaktion auf sicherheitsrelevante Ereignisse und Schwachstellen**
    Wie wird auf unerwartete Ereignisse reagiert? Sollte ein Ereignis eintreten, sollte bekannt sein, wie dieses behandelt wird.

- **Physische Sicherheit**
  - **Sicherheitsbereiche**
    Welches sind besonders schützenswerte Bereiche? Dazu zählt zum Beispiel der Serverraum.
  - **Verkabelung, Wireless LAN**
    Die Verkabelung gehört ebenfalls in die physische Sicherheit. Kabel sollten nicht durch ungeschützte Bereiche führen. Auch kabellose Netzwerke sind in die Planung aufzunehmen.

- **Betrieb von Systemen und Netzwerken**
  - **Operative Verfahren und Aufgaben**
    Daily-Business der Administratoren: Welche Dienste und Protokollierungen sind regelmässig zu kontrollieren?
  - **Systemplanung und -abnahme**
    Neue Systeme sind auf die Verträglichkeit mit den bestehenden Mitteln zu testen. Dazu gehört ein Kontroll- und Abnahmeverfahren.
  - **Systemverwaltung**
    Systeme werden regelmässig angepasst (zum Beispiel durch Patches, Updates, neue Versionen). Alle Änderungen sind zu protokollieren.
  - **Internet**
    Das Internet ist eine ideale Informationsquelle. Ebenso leicht ist es, unerwünschte Software einzuschleusen. Die gewählten Massnahmen sind festzuhalten und zu kommunizieren.
  - **Schutz gegen Malware**
    Der Schutz davor muss durch ein mehrstufiges Verfahren sichergestellt werden.

- **Zugriffskontrolle**
  - **Benutzer Administration**
    Dieser Punkt behandelt die Art der Identifikation, der Kontrolle und der Administration der Benutzer (Gruppen, Rechte, Vergabe und Einschränkungen)
  - **Betriebssystem-Zugriffskontrolle**
    Wie wird der Zugriff auf das System geregelt? Wie werden die Zugriffe kontrolliert?
  - **Einsatz mobiler Geräte**
    Mobile Geräte sind sehr schwer zu kontrollieren, da sie oft unterwegs sind. Bevor sie jedoch an das Firmennetz angeschlossen werden, müssen verschiedene Kontrollen stattfinden (Patches oder Malware)

- **Unterhalt von Informationssystemen**
  - **Änderungswesen**
    Änderungen an Systemen und Abläufen sind schriftlich festzuhalten, zum Beispiel in einem Logbuch.

- **Not-Organisation**
  - Welche Mittel sind für einen eingeschränkten Betrieb notwendig? Gibt es Ausweichmöglichkeiten (andere Gebäude, Lieferanten- und Wartungsverträge)?

- **Einhaltung und Überprüfung der Aufgaben**
  - **Konformität mit gesetzlichen Angaben**
    Gesetzlichen Anforderungen müssen bekannt sein und eingehalten werden
  - Überprüfung der Sicherheitspolitik und der technischen Konformität
    Regelmässige Überprüfungen durch interne und externe Stellen gewährleisten, dass das Konzept aktuell und komplett ist.

- **Anhänge**
  - Gefährdung und Risikoanalyse Inkl. Restrisiken
  - IT-Strategie und -Organisation
  - Betrieb der IT-Struktur
  - Nutzung von PC, Netzwerk und Online-Diensten
  - Nutzung von Hard- und Software
  - Backup-Konzept
  - Backup-Plan
  - Firewall-Konzept
  - Akzeptierte Ausfallzeiten und Not-Organisation

Verantwortlichkeiten sind klar zu definieren.

Sobald Massnahmen für die einzelnen Bereiche definiert wurden, gilt es, diese zusammenzufassen und Synergien zu finden.

Wirtschaftlichkeit einbeziehen
Schlussendlich dreht sich alles um das Geld. Kann und will ich mir diesen Schutz leisten? Es ist wichtig zu definieren, welchen Schaden eine Gefährdung anrichten kann. Teilen Sie die Auswirkungen in Kategorien von niedriger bis mittlerer Schaden, hoher Schaden und sehr hoher Schaden ein. Dort, wo der Schaden am grössten ist, sollten die ersten Massnahmen umgesetzt werden.

Allerdings: Nicht alle Massnahmen können umgesetzt werden. Dieses Restrisiko muss bewusst durch die Geschäftsleitung getragen werden.

Strategisches Vorgehen
Mit den Antworten auf diese vier Fragen kann das weitere Vorgehen definiert werden. Die Resultate sind zu bewerten und detailliert auszuarbeiten. Damit verbunden sind die finanziellen und personellen Aufwände. Mit der Auswahl der Massnahmen kann auch die Reihenfolge definiert werden. Welche Massnahmen sind zeitkritisch? Welche Massnahmen lassen sich auch später noch realisieren? Was konsolidiert werden kann, sollte auch gleichzeitig umgesetzt werden.

Der wichtigste Punkt bei der Umsetzung sind die Verantwortlichkeiten. Wer trägt die Verantwortung für eine Massnahme? Nur wer sich verpflichtet fühlt, wird auch das Zepter in der Hand halten.

Gleichzeitig mit der Umsetzung stellen begleitende Massnahmen einen wichtigen Handlungsrahmen dar. Die Schulung und die Sensibilisierung von Mitarbeitern sind wichtig. Die Mitarbeiter müssen genug früh auf die Umstellungen vorbereitet werden, um möglichen Missverständnissen vorzubeugen.

Verantwortung festlegen
Eine regelmässige Kontrolle ist notwendig, um Abweichungen und veränderte Bedingungen zu erkennen und Anpassungen zu treffen. Die Verantwortlichkeiten sind entsprechend festzuhalten.

Sollte es zu Änderungen kommen, ist das Management miteinzubeziehen und die entscheidenden Schritte zu treffen. Denken Sie auch hier daran, frühzeitig alle Mitarbeiter über die veränderten Situationen zu orientieren.

Zusammenfassung
Ein IT-Sicherheitskonzept ist nicht in einem Tag erstellt. Die Vorbereitungsarbeiten nehmen viel Zeit in Anspruch. Doch diese Zeit lohnt sich. Massnahmen, die sich auf kritische Systeme auswirken, sollten anschliessend im ersten Schritt umgesetzt werden. Halten Sie fest, wer die Verantwortung für die Umsetzung und Kontrolle von Massnahmen trägt.

Während und nach der Umsetzung gilt es, die Massnahmen zu kontrollieren, sei dies durch interne oder externe Stellen.

Schulen und sensibilisieren Sie alle Stufen, von der Geschäftsleitung bis zum Mitarbeiter. So wird auch Ihr Konzept zum Erfolg! ■

Andreas Wisler

(CISSP, CISA, ISO 22301 + 27001 Lead-Auditor) ist Geschäftsführer und Senior-Security-Auditor bei der goSecurity GmbH, welche IT-Sicherheitsüberprüfungen und -beratungen durchführt. Weiter unterrichtet er unter anderem an der Fachhochschule Nordwestschweiz FHNW IT-Sicherheitsthemen.